CLAIM AMENDMENTS

Claim Amendment Summary

Claims pending

- Before this Amendment: Claims 1-5, 7-8, and 10-34
- After this Amendment: Claims 1-5, 7-8, 10, and 23-34

Non-Elected, Canceled, or Withdrawn claims: 11-22

Amended claims: 2-4 and 7

New claims: None

Claims:

1. (Previously Presented) A method of file system protection for a resource-sparing operating system image, comprising:

loading, with a client computing device, a first image of the resource-sparing operating system (OS) that includes processor instructions into random access memory (RAM), the first image including an embedded second image of a catalog file comprising client device attributes;

creating, with the client computing device, a first hash of the first image;

extracting with the client computing device a second hash from the second image of the catalog file;

comparing with the client computing device the first hash and the second hash; and

validating with the client computing device the use of the first image to boot the computing device if the first hash and the second hash match.

2. (Currently Amended) The method of claim 1, wherein the comparing includes determining that the first hash and the second hash do not match[[,]] and ~~wherein further the~~ blocking the use of the first image to boot the computing device if the first hash and the second hash do not match comprising[[es]] determining that an operational mode of the computing device is set to a run mode of operation.

3. (Currently Amended) The method of claim 1, wherein the comparing includes determining that the first hash and the second hash match, and wherein ~~further~~ the validating the use of the first image to boot the computing device if the first hash and the second hash match further includes validating a signature certification of the first image.

4. (Currently Amended) The method of claim 1, further comprising:

evaluating a signature certification of the catalog file in the second image to determine if the signature certification of the catalog file is valid[[,]] and ~~wherein the~~ blocking the use of the first image to boot the computing device if the first hash and the second hash do not match ~~further~~ including[[es]] blocking the use of the first image to boot the computing device if the signature certification of the catalog file cannot be validated.

5. (Previously Presented) The method of claim 4, further comprising determining whether an operational mode of the computing device is set to a run mode of operation.

6. (Canceled)

7. (Currently Amended) The method of claim 1, further comprising:

extracting first make and model attributes from the second image of the catalog file, comparing the first make and model attributes from the second image of the catalog file with second make and model attributes of the computing device, and ~~wherein the~~ blocking the use of the first image to boot the computing device if the first hash and the second hash do not match ~~further~~ including[[es]] blocking the use of the first image to boot the computing device if the first make and model attributes do not match the second make and model attributes.

8. (Previously Presented) The method of claim 7, further comprising determining whether an operational mode of the computing device is set to a run mode of operation.

9. (Canceled)

10. (Previously Presented) The method of claim 1, further comprising booting the computing device from a third image of a prior resource-sparing OS already loaded in flash memory of the computing device.

11-22. (Cancelled)

23. (Previously Presented) A portable computing device, comprising:

flash memory, the flash memory including a protected area and an unprotected area;

a bootloader stored in the protected area of flash memory, the bootloader containing a cryptographic module;

an operating system (OS) image installed in the unprotected area of flash memory;

random access memory (RAM); and

wherein the cryptographic module of the bootloader is operative to examine an update image to the OS image to determine if the update image should be programmed into the unprotected area of flash memory to boot the computing device, wherein a signed catalog image is an image of a signed catalog file and is embedded in the update image, wherein the signed catalog file is derived by signing a catalog file, and wherein the cryptographic module is operative to program the update image into the unprotected area of flash memory boot the computing device based on a determined relationship between information extracted from the embedded signed catalog file and one of

information about the components of the computing device and information determined from the update image.

24. (Previously Presented) The device of claim 23, wherein the cryptographic module programs the update image into the unprotected area of flash memory when the device is in test mode.

25. (Previously Presented) The device of claim 23, wherein the bootloader stores the update image in the RAM until the cryptographic module determines that the update image should be programmed into the unprotected area of flash memory to boot the device.

26. (Previously Presented) The device of claim 25, wherein the cryptographic module calculates a first hash of the update image, extracts a second hash from the catalog file image, and compares the first hash and the second hash, the cryptographic module blocking use of the update image when the first hash and the second hash do not match.

27. (Previously Presented) The device of claim 25, wherein the cryptographic module extracts a signature certification from the catalog file and attempts to validate the signature certification, the cryptographic module blocking use of the OS image update when the signature certification cannot be validated.

28. (Previously Presented) The device of claim 25, wherein the operating system (OS) image is an image of an operating system, wherein the update image is an image of an update file to the OS, wherein the cryptographic module is operative to program the update image into the unprotected area of flash memory boot the computing device based on a determined relationship between information extracted from the signed catalog file and information about the components of the computing device by:

extracting make and model attributes from the catalog file and comparing them to make and model information for the computing device, and

blocking use of the update image when the make and model attributes of the catalog file do not match the make and model attributes of the computing device.

29. (Previously Presented) The device of claim 25, wherein the bootloader erases a current device image from the unprotected area of flash memory and programs the update image into the unprotected area of flash memory when the cryptographic modules determines that the update image may be used to boot the device.

30. (Previously Presented) The device of claim 23, wherein a second cryptographic module of a Mira shell is operative upon a reset of the computing device to examine the installed operating system image to determine if the installed operating system image should be used to boot the computing device based on information included in the signed catalog file.

31. (Previously Presented) The device of computing claim 30, wherein the cryptographic module in the Mira shell calculates a first hash of the installed operating system image, extracts a second hash from the catalog image, and compares the first hash and the second hash, the cryptographic module in the Mira shell blocking use of the update image when the first hash and the second hash do not match.

32. (Previously Presented) The device of computing claim 30, wherein the cryptographic module in the Mira shell extracts a signature certification from the catalog file and attempts to validate the signature certification, the cryptographic module in the Mira shell blocking use of the installed operating system image when the signature certification cannot be validated.

33. (Previously Presented) The computing device of claim 30, wherein the cryptographic module in the Mira shell extracts make and model attributes from the catalog file and compares them to make and model information for the computing device, wherein the operating system image is an image of an operating system for the computing device, the cryptographic module in the Mira shell blocking use of the installed operating system image when the make and model attributes of the installed operating system do not match the make and model attributes of the computing device.

34. (Previously Presented) The computing device of claim 30, wherein the cryptographic module in the Mira shell allows the installed operating system image to be used to boot the computing device when the computing device is in test mode.